PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-084049

(43)Date of publication of application : 30.03.2001

(51)Int.Cl. G06F 1/00
G06F 13/14

(21)Application number : 11-256243

(22)Date of filing : 09.09.1999

(71)Applicant : CANON INC

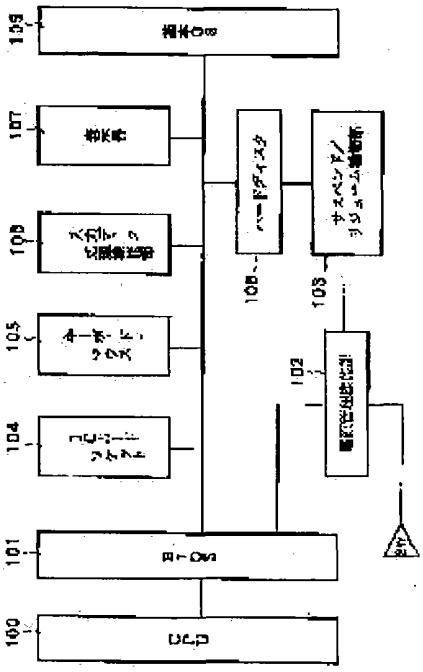
(72)Inventor : OKA KOJI

(54) COMPUTER AND SECURITY METHOD FOR COMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a computer and a computer security method capable of solving problems such as the processing load of a CPU and suitably protecting the computer.

SOLUTION: In the computer having an IC card socket 104 as a security device, a BIOS 101 judges whether the computer is to be protected or not on the basis of the inserted/ejected state of an IC card into/from the socket 104, and at the time of judging the necessity of protection, inhibits the processing of all or a part of hardware 105 or the like. Since the hardware 105 is directly controlled by the BIOS 101, the use of the computer body can be disabled and sure security measures can be applied to third persons.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－84049
（P2001－84049A）
(43)公開日　平成13年３月30日(2001.3.30)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ　1/00	３７０Ｅ	５Ｂ０１４
13/14	３３０	13/14	３３０Ｄ	

審査請求　未請求　請求項の数21　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－256243

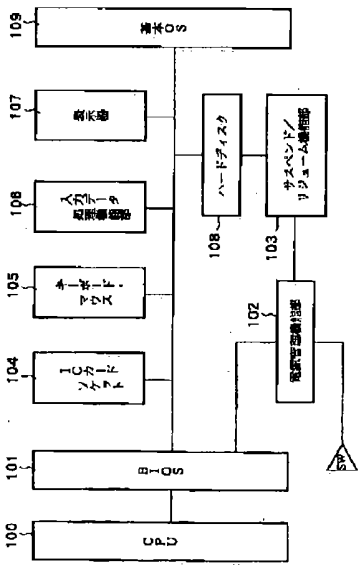
(22)出願日　平成11年９月９日(1999.9.9)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　岡　弘次
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100076428
弁理士　大塚　康徳　（外２名）

Ｆターム(参考)　5B014 HB04 HC03 HC06

(54)【発明の名称】　コンピュータ及びコンピュータのセキュリティ方法

(57)【要約】
【課題】　ＣＰＵの処理負担等の問題を解決し、コンピュータを好適に保護し得るコンピュータ及びコンピュータのセキュリティ方法を提供すること。
【解決手段】　セキュリティデバイスとしてのＩＣカードソケット１０４を有するコンピュータであって、ＢＩＯＳ１０１が、ＩＣカードソケット１０４に対するＩＣカードの挿脱の状態に基づいて、コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、全部又は一部のハードウエア１０５等の処理を禁止する。ＢＩＯＳによりハードウェアを直接コントロールすることで、コンピュータ本体を使用不能にすることを可能にし、第三者に対し強固なセキュリティ対策を施すことができる。



【特許請求の範囲】
【請求項１】　セキュリティデバイスを有するコンピュータであって、
前記コンピュータのＢＩＯＳが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウエアの処理を禁止することを特徴とするコンピュータ。
【請求項２】　前記セキュリティデバイスが、ＩＣカードと当該ＩＣカードを挿入するためのソケットと、からなり、
前記ＢＩＯＳは、前記ＩＣカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定することを特徴とする請求項１に記載のコンピュータ。
【請求項３】　前記ＢＩＯＳは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウエアの処理を禁止することを特徴とする請求項１に記載のコンピュータ。
【請求項４】　前記ＢＩＯＳは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止することを特徴とする請求項１に記載のコンピュータ。
【請求項５】　前記ＢＩＯＳは、保護の必要があると判定した場合は、ディスプレイの表示を禁止することを特徴とする請求項１に記載のコンピュータ。
【請求項６】　前記ＢＩＯＳは、保護の必要があると判定した場合は、電源のＯＮ／ＯＦＦを禁止することを特徴とする請求項１に記載のコンピュータ。
【請求項７】　前記ＢＩＯＳは、前記ＩＣカードが、前記ソケットに挿入されている場合は、電源のＯＦＦを禁止することを特徴とする請求項２に記載のコンピュータ。
【請求項８】　セキュリティデバイスを有するコンピュータのセキュリティ方法であって、
前記コンピュータのＢＩＯＳが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウエアの処理を禁止することを特徴とするコンピュータのセキュリティ方法。
【請求項９】　前記セキュリティデバイスが、ＩＣカードと当該ＩＣカードを挿入するためのソケットと、からなり、
前記ＢＩＯＳは、前記ＩＣカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定することを特徴とする請求項８に記載のコンピュータのセキュリティ方法。
【請求項１０】　前記ＢＩＯＳは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウエアの処理を禁止することを特徴とする請求項８に記載のコンピュータのセキュリティ方法。
【請求項１１】　前記ＢＩＯＳは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止することを特徴とする請求項８に記載のコンピュータのセキュリティ方法。
【請求項１２】　前記ＢＩＯＳは、保護の必要があると判定した場合は、ディスプレイの表示を禁止することを特徴とする請求項８に記載のコンピュータのセキュリティ方法。
【請求項１３】　前記ＢＩＯＳは、保護の必要があると判定した場合は、電源のＯＮ／ＯＦＦを禁止することを特徴とする請求項８に記載のコンピュータのセキュリティ方法。
【請求項１４】　前記ＢＩＯＳは、前記ＩＣカードが、前記ソケットに挿入されている場合は、電源のＯＦＦを禁止することを特徴とする請求項９に記載のコンピュータのセキュリティ方法。
【請求項１５】　セキュリティデバイスを有するコンピュータのＢＩＯＳのプログラムを記録した記憶媒体であって、該プログラムが、
前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウエアの処理を禁止するプログラムであることを特徴とする記憶媒体。
【請求項１６】　前記セキュリティデバイスが、ＩＣカードと当該ＩＣカードを挿入するためのソケットと、からなり、
前記プログラムは、前記ＩＣカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定するプログラムを含むことを特徴とする請求項１５に記載の記憶媒体。
【請求項１７】　前記プログラムは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウエアの処理を禁止するプログラムを含むことを特徴とする請求項１５に記載の記憶媒体。
【請求項１８】　前記プログラムは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止するプログラムを含むことを特徴とする請求項１５に記載の記憶媒体。
【請求項１９】　前記プログラムは、保護の必要があると判定した場合は、ディスプレイの表示を禁止するプログラムを含むことを特徴とする請求項１５に記載の記憶媒体。
【請求項２０】　前記プログラムは、保護の必要があると判定した場合は、電源のＯＮ／ＯＦＦを禁止するプログラムを含むことを特徴とする請求項１５に記載の記憶媒体。
【請求項２１】　前記プログラムは、前記ＩＣカードが、前記ソケットに挿入されている場合は、電源のＯＦ

Ｆを禁止するプログラムを含むことを特徴とする請求項１６に記載の記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デスクトップ及びノートブックパソコン、サーバーコンピュータ、若しくは同サーバーに接続するワークステーション等のコンピュータ機器に対するセキュリティシステムに関するものである。

【０００２】

【従来の技術】第三者がコンピュータを無断で操作できないように、コンピュータのセキュリティシステムが提案されている。このセキュリティシステムでは、例えば、ＰＣＭＣＩＡソケット或いは同様の専用ソケットをコンピュータに設け、そこにＩＣカードが挿入されたか否かにより、正当な者の利用か否かを区別するものである。

【０００３】そして、従来、ＩＣカードによるセキュリティは基本的にはソフトウェアによる保護対策であり、例えばＩＣカードが抜かれた場合に、あらかじめ定めた特定のアプリケーションを、ＩＣカードに関連付けられたセキュリティソフトによって利用不可能にするか、同セキュリティソフトによって表示画面全体をモザイク化して判読不能する等のソフト処理を行うものである。

【０００４】これらは、セキュリティ対象のアプリケーションとセキュリティソフトの仕掛けによって行われており、再度使用するにはカード挿入後にパスワードを入力し、操作者の正当性を認識しセキュリティソフトによる解除を行うようにしていたのが現状である。

【０００５】

【発明が解決しようとする課題】しかしながら、上記従来の方法では、ＩＣカードに関連付けられたソフトウェアを常時起動しておく必要性からメモリを常に占有されるという問題がある。また、ソフトによるＩＣカードの抜き差しを定期的にソケットサービスプログラムに対し割り込み処理を使って交信することからＣＰＵの負荷が大きくなり、その他の処理に遅延が発生するという問題がある。更に、特定のアプリケーションに対しての処理である為、パソコン本体は使用可能であり、その他のアプリケーションや資産は保護されていない等の問題がある。

【０００６】従って、本発明の目的は、係る問題を解消し、コンピュータを好適に保護し得るコンピュータ及びコンピュータのセキュリティ方法を提供することにある。

【０００７】

【課題を解決するための手段】本発明によれば、セキュリティデバイスを有するコンピュータであって、前記コンピュータのＢＩＯＳが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウエアの処理を禁止することを特徴とするコンピュータが提供される。

【０００８】本発明においては、前記セキュリティデバイスが、ＩＣカードと当該ＩＣカードを挿入するためのソケットと、からなり、前記ＢＩＯＳは、前記ＩＣカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定することもできる。この場合、前記ＢＩＯＳは、前記ＩＣカードが、前記ソケットに挿入されている場合は、電源のＯＦＦを禁止することもできる。

【０００９】また、本発明においては、前記ＢＩＯＳは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウエアの処理を禁止することもできる。

【００１０】また、本発明においては、前記ＢＩＯＳは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止することもできる。

【００１１】また、本発明においては、前記ＢＩＯＳは、保護の必要があると判定した場合は、ディスプレイの表示を禁止することもできる。

【００１２】また、本発明においては、前記ＢＩＯＳは、保護の必要があると判定した場合は、電源のＯＮ／ＯＦＦを禁止することもできる。

【００１３】また、本発明によれば、セキュリティデバイスを有するコンピュータのセキュリティ方法であって、前記コンピュータのＢＩＯＳが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウエアの処理を禁止することを特徴とするコンピュータのセキュリティ方法が提供される。

【００１４】また、本発明によれば、セキュリティデバイスを有するコンピュータのＢＩＯＳのプログラムを記録した記憶媒体であって、該プログラムが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウエアの処理を禁止するプログラムであることを特徴とする記憶媒体が提供される。

【００１５】

【発明の実施の形態】以下、本発明の好適な実施の形態について、図面を参照して詳細に説明する。

【００１６】図１は、本発明の一実施形態に係るコンピュータのブロック図である。

【００１７】図１のコンピュータは、ＣＰＵ１００、ＢＩＯＳ（基本入出力システム）１０１、電源管理機能部１０２、サスペンド／リジューム機能部１０３、セキュリティＩＣカードを挿抜するソケット１０４、キーボード或はマウスポインタ等の入力機器１０５、入力データ

処理機能部１０６、表示器１０７、ハードディスク１０８、基本ＯＳ１０９を備える。なお、特に図示するものではないが、ＣＰＵ１００により参照、実行されるプログラムの配置される実行メモリ領域や、ＣＰＵ１００の作業領域、１０９基本ＯＳ、或いはＯＳ上で動作するプログラム等が、データを一時的に格納する記憶メモリ領域等のＲＡＭ、外部記憶媒体はもちろん備えている。

【００１８】図２は、ＩＣカードコネクタとカードソケットの一般的な回路の例を示した図である。

【００１９】図中、２００はＩＣカードコネクター、２０１は接続信号線、２０２はカードソケット、２０３はソケット側の接続信号線、２０４は接続を認識し信号をｈｉｇｈに維持するＶＣＣ、２０５は割り込み信号線、２０６はリセット信号線、２０７はクロックリセット、である。

【００２０】図２には明記していないが、ＩＣカードがセキュリティカードか否かを判断する手段は、カードソケット及びＩＣカードコネクタに専用の信号線を用意し、その信号線からの信号を認識する手段、或いはセキュリティ専用ソケットを用いても問題はなく、何ら限定するものではない。

【００２１】以下、図２と図３とを用いてＩＣカードの挿抜による信号の変化を説明する。図３は、ＩＣカードの挿抜時のソケット１０４からの信号（以下、ソケット信号ともいう。）の状態と、電源管理機能部１０２が作動するタイミングを示した図である。

【００２２】図３において、３００はソケット２０２のカード認識による信号の変化を、３０１は割り込み信号の変化を、３０２はリセット信号の変化を、それぞれ示している。

【００２３】操作者がＩＣカードをタイミング３００ａで挿入した場合に、タイミング３０１ａでＶＣＣは信号をｌｏｗに落としカード認識を示す。割り込み回路は同信号を認識すると割り込み信号をｈｉｇｈにセットし、割り込み要求を出す。

【００２４】割り込み要求により、任意の処理が実行された後、タイミング３０２ａで割り込み信号をリセットし、チェックリセットは割り込み信号を落とす。

【００２５】次に、タイミング３００ｂで操作者がＩＣカードを取り出すと、ＶＣＣは信号をｈｉｇｈにセットしカードの取りだしを認識する。同信号を認識すると、割り込み回路はタイミング３０１ｂで割り込み信号をｈｉｇｈにセットし、割り込み要求を出す。割り込み要求により、任意の処理が実行された後、タイミング３０２ｂで割り込み信号をリセットし、チェックリセットは割り込み信号を落とす。

【００２６】次に、係る構成からなるコンピュータにおいて実行される処理について説明する。

＜処理１＞ここでは、ＩＣカードの抜き差しによつて、全メモリ上の内容をＨＤＤや所定のＲＡＭ上に設けられたサスペンド領域（退避領域）に格納し、パソコン本体を停止状態にする場合を述べる。図４および図５は、係る処理のフローチャートである。なお、この例では、セキュリティＩＣカードが挿入された場合、ソケット信号をｌｏｗとし、非挿入時の同信号をｈｉｇｈとする。

【００２７】まず、ＩＣカードが抜かれると、ソケット信号がｈｉｇｈにセットされ（ステップＳ４００）、ステップＳ４０１において割り込み信号をｈｉｇｈにセットして割り込み要求を出す。本実施形態では電源管理機能部１０２が割り込みを認識し、ＢＩＯＳ１０１に対しサスペンド処理のイベントを発する。

【００２８】ステップＳ４０２では、ＢＩＯＳ１０１はイベントの発生によりサスペンド機能を起動し、全メモリ上のデータをＨＤＤ１０８上に設けた退避領域、或いは退避用に設けた専用ＲＡＭ（図示しない）に保管し、ステップＳ４０３でサスペンドフラグをＯＮにする。更に、ステップＳ４０４において割り込み回路で設定された信号をｌｏｗにリセットして電源を落とす。

【００２９】次に、図５を参照して、ステップＳ５００において電源が投入されると、ステップＳ５０１で電源管理機能部１０２は、ソケット信号を確認する。

【００３０】ステップＳ５０２では、信号がｈｉｇｈかｌｏｗかを判定し、ｌｏｗならばＩＣカードが挿入されていると判断してステップＳ５０３で電源管理機能部１０２は割り込み信号をｈｉｇｈにセットし、ＢＩＯＳに制御を渡す。ｈｉｇｈならばステップＳ５００へ戻る。

【００３１】次に、ステップＳ５０４において、ＢＩＯＳ１０１がイベント発生を感知したらサスペンドフラクを参照し、ＯＮならばサスペンド状態であると判断しリジューム処理（復元処理）を行う。その後、サスペンドフラグをリセットし（ステップＳ５０５）、また、割り込み信号をリセット（ステップＳ５０６）して通常の処理へ至る。なお、特に明記はしないが、上記サスペンド及びリジューム処理例は、一般的な公知の方法で問題はない。

【００３２】以上述べたようにＩＣカードが抜かれた場合にパソコン自体を休止状態にすること、及び再度挿入された場合には休止状態以前の状態に復元することでパソコンを第三者に使用させることを禁止する効果があるばかりか、作業途中の状態を維持したまま保護対策を実施できる効果がある。

＜処理２＞この処理では、ＩＣカードの抜き差しによって、キーボード及びマウス等の入力機器１０５からのデータをコントロールすることによって、パソコン本体を使用不能状態にする場合を述べる。図６および図７は、係る処理のフローチャートである。

【００３３】この例では、セキュリティＩＣカードが挿入された場合のソケット信号をｌｏｗとし、非挿入時の同信号をｈｉｇｈとして述べる。

【００３４】ＩＣカードが抜かれると、ソケット信号が

ｈｉｇｈにセットされ（ステップＳ６００）、割り込み要求を出す（ステップＳ６０１）。
【００３５】ステップＳ６０２では、ＢＩＯＳ１０１が割り込みイベントの発生を認識し、入力データ処理機能部１０６に対しデータ取得を停止させる。これにより、キーボード・マウス１０５からの入力は、無効になる。その後、ステップＳ６０３において割り込み回路からの信号をリセットする。
【００３６】次に、図７を参照して、ステップＳ７００は、ＩＣカードが挿入されたことを意味している。ステップＳ７０１では、ＶＣＣによる挿入信号を電源管理機能部１０２が認識し、ステップＳ７０２において、該信号をｈｉｇｈかｌｏｗかを判定する。ｌｏｗであればステップＳ７００へ戻り、ｈｉｇｈならば、ステップＳ７０３において、割り込み要求を出す。
【００３７】ＢＩＯＳ１０１は、割り込みイベントを確認すると、ステップＳ７０４において入力データ処理機能部１０６に対しデータ取得処理を再開させる。これによりキーボード・マウス１０５からの入力が有効になる。その後、ステップＳ７０５で割り込み信号をリセットする。
【００３８】以上述べたようにＩＣカードが抜かれた場合にＢＩＯＳに対し、キーボードやマウスからの入力データ取得を停止し、再度挿入されている場合にのみ入力データを処理することでパソコン自体を使用不可能にし、第三者からの保護対策として効果がある。
＜処理３＞この例ではＩＣカードの抜き差しによって、表示器への出力信号をコントロールし、表示画面を消しパソコン本体を使用不能にする場合を述べる。図８および図９は、係る処理のフローチャートである。なお、この例では、ＩＣカードが挿入された場合のソケット信号をｌｏｗとし、非挿入時の同信号をｈｉｇｈとして述べる。
【００３９】ＩＣカードが抜かれると、ステップＳ８００においてソケット信号がｈｉｇｈにセットされ、ステップＳ８０１で電源管理機能部１０２は割り込み信号をｈｉｇｈにセットし割り込み要求を出す。
【００４０】ステップＳ８０２においてＢＩＯＳ１０１は割り込みイベントの発生を認識し、図示しない表示機能部に対し表示器１０７への出力信号を停止させる。これにより、表示器１０７の表示内容が不変となる。その後、ステップＳ８０３で割り込み回路からの信号をリセットし、待機状態になる（ステップＳ８０４）。
【００４１】次に、図９を参照して、ステップＳ９００は、ＩＣカードが挿入されたことを意味している。ステップＳ９０１で，ソケット信号が確認される。ステップＳ９０２において、ソケット信号がｌｏｗの場合はステップＳ９００へ戻り、信号がｈｉｇｈの場合は、電源管理機能部１０２が割り込み信号をｈｉｇｈにセットし割り込み要求を出す（ステップＳ９０３）。
【００４２】ステップＳ９０４では、ＢＩＯＳ１０１は割り込みイベントの発生を認識し、表示機能部に対し表示器１０７への信号出力を再開させる。これにより表示器１０７の表示内容が可変となる。その後、割り込み信号をリセットする（ステップＳ９０５）。
【００４３】以上述べたようにＩＣカードが挿入されている場合にのみ、表示器への信号を出力するため、操作者がしばらくパソコンを放置する際に、ＩＣカードを抜くだけで画面上の表示内容を消去し、第三者に対し保護対策としての効果がある。
＜処理４＞この例では、ＩＣカードの抜き差しによって、電源管理機能部１０２をコントロールすることによって、ＩＣカードが挿入された場合に電源が供給され、ＩＣカードが挿入されている場合にのみ電源の切断が行えるようにする場合を述べる。図１０と図１１は、係る処理のフローチャートである。この例では、セキュリティＩＣカードが挿入された場合のソケット信号をｌｏｗとし、非挿入時の同信号をｈｉｇｈとして述べる。
【００４４】ステップＳ１０００は、コンピュータの電源が投入されたことを示している。ステップＳ１００１では、カードソケット２０２がＩＣカードの挿入を確認後、信号をｌｏｗにセットする。
【００４５】ステップＳ１００２では、電源管理機能部１０２はソケット信号がｌｏｗになるのを待ち、ｌｏｗになった時点で電力を供給し、以降の通常のコンピュータ起動処理をＢＩＯＳ管理下で行う（ステップＳ１００３及びＳ１００４）。即ち、ＩＣカードが挿入されていることを認識したら電源を供給する。
【００４６】次に、図１１を参照して、ステップＳ１１００は、電源の切断操作が行われたことを意味している。ステップＳ１１０１において、電源管理機能部１０２はソケット信号を参照し、ステップＳ１１０２においてｌｏｗを確認したら、ステップＳ１１０３で割り込み信号をセットし、システム終了（ステップＳ１１０５）及び割り込み信号のリセット（ステップＳ１１０６）の後、電源を遮断する。即ち、ＩＣカードが挿入されていることを認識したら電源遮断を行う。その後、ステップＳ１１０６で割り込み信号をリセットする。
【００４７】ここでＩＣカードが抜かれている時点で電源の切断操作が行われた場合、ソケット信号（ｈｉｇｈ）を認識したら、操作者にＩＣカード挿入を要求するメッセージを出力することもできる（ステップＳ１１０４）。その方法は表示メッセージ或いは警告音や警告メッセージ等があるが何ら限定するものではない。
【００４８】以上述べたようにセキュリティＩＣカードが挿入されている場合にのみパソコンの使用を可能にし、パソコンを同ＩＣカードを持たない第三者に使用させることを禁止する効果がある。
【００４９】なお、上記処理４の例ではＩＣカードの挿入時のみ、電源のＯＮ／ＯＦＦを行えるようにし、パソ

コンの使用を第三者に対し禁止する手段であったが、電源ＯＦＦ後、ＩＣカードの抜き忘れが発生し第三者に利用される不具合がある。

【００５０】その対策として、ＩＣカードが挿入された場合に電源が供給され、ＩＣカードが抜かれている場合にのみ電源の切断が行えるようにする場合を述べる。図１２は、係る処理のフローチャートである。この例では、ＩＣカードが挿入された場合のソケット信号をｌｏｗとし、非挿入時の同信号をｈｉｇｈとして述べる。

【００５１】ステップＳ１２００は、電源の切断操作が行われたことを意味している。ステップＳ１２０１において電源管理機能部１０２はソケット信号を参照し、ステップＳ１２０２においてｈｉｇｈにセットされていることを認識した場合、すなわちＩＣカードが抜かれていることを認識した場合は、ステップＳ１２０３において割り込み信号をｈｉｇｈにセットする。その後、システムの終了（ステップＳ１２０５）及び割り込み信号をリセット（ステップＳ１１０６）して、電源を遮断する。

【００５２】ここでＩＣカードが挿入されている時点で電源の切断操作が行われた場合、ソケット信号ｌｏｗを認識したら、ステップＳ１２０４において電源管理機能部１０２は操作者にＩＣカード取りだしを要求するメッセージを出力する。その方法は表示メッセージ或いは警告音や警告メッセージ等があるが何ら限定するものではない。

【００５３】以上、本発明の好適な実施の形態について説明したが、上述した処理の例は、それぞれ組み合わせて用いることができることはいうまでもない。

【００５４】なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５５】

【発明の効果】以上説明したように本発明によれば、ＢＩＯＳによりハードウェアを直接コントロールすることで、コンピュータ本体を使用不能にすることを可能にし、第三者に対し強固なセキュリティ対策を施すことができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンピュータの構成を示すブロック図である。

【図２】ＩＣカードコネクタとカードソケットの一般的な回路の例を示した図である。

【図３】ＩＣカードの挿抜時のソケット１０４からの信号の状態と、電源管理機能部１０２が作動するタイミングを示した図である。

【図４】本発明の一実施形態における処理１のフローチャートである。

【図５】本発明の一実施形態における処理１のフローチャートである。

【図６】本発明の一実施形態における処理２のフローチャートである。

【図７】本発明の一実施形態における処理２のフローチャートである。

【図８】本発明の一実施形態における処理３のフローチャートである。

【図９】本発明の一実施形態における処理３のフローチャートである。

【図１０】本発明の一実施形態における処理４のフローチャートである。

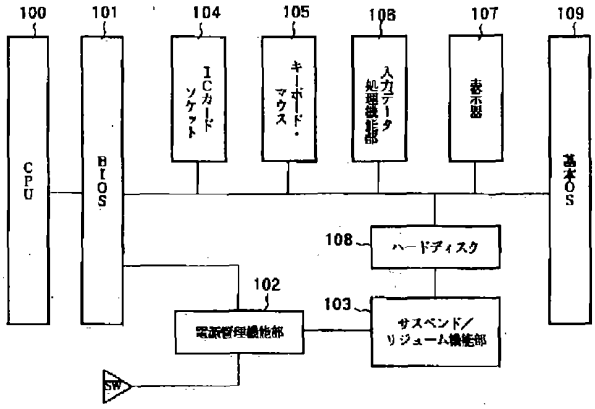
【図１１】本発明の一実施形態における処理４のフローチャートである。

【図１２】本発明の一実施形態における処理４のフローチャートである。

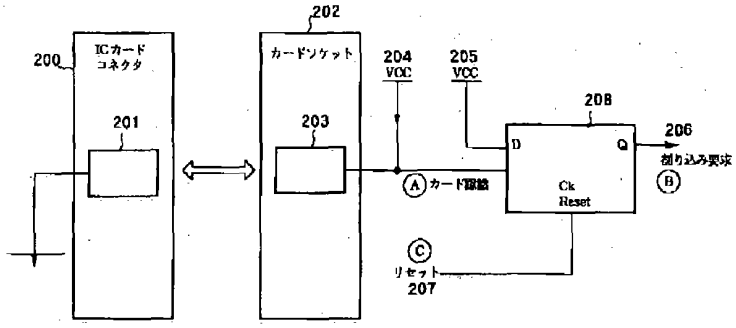
【符号の説明】

１００　ＣＰＵ
１０１　ＢＩＯＳ
１０２　機能部
１０３　サスペンド／リジューム機能部
１０４　ＩＣカードソケット
１０５　キーボード或はマウス
１０６　入力データ処理機能部
１０７　表示器
１０８　ハードディスク
１０９　基本ＯＳ

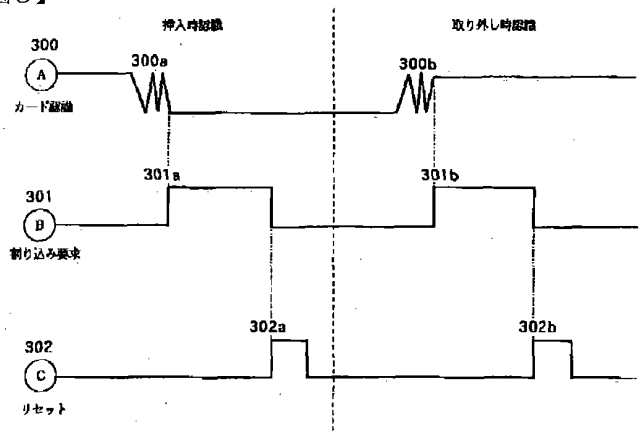
【図１】


100
101
104
105
108
107
109
CPU
BIOS
ICカードソケット
キーボード・マウス
入力データ処理機能部
表示器
基本OS
108
ハードディスク
102
103
電源管理機能部
サスペンド/リジューム機能部
SW

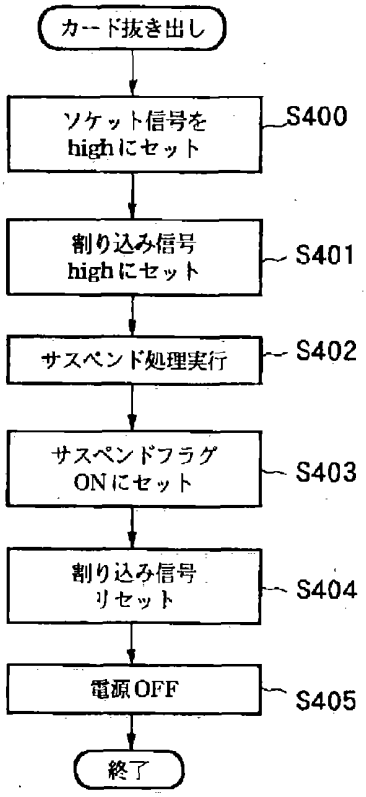
【図２】


202
200
ICカードコネクタ
カードソケット
204
VCC
205
VCC
208
201
203
D
Q
206
割り込み要求
Ck
Reset
Ⓐ カード認識
Ⓑ
Ⓒ
リセット
207

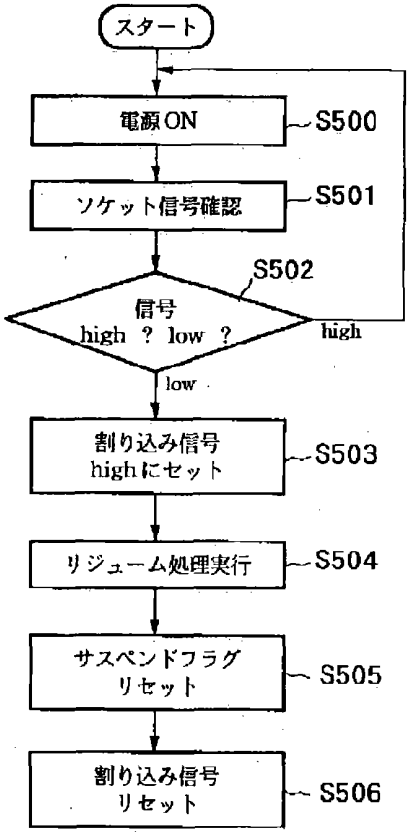
【図３】


挿入時認識
取り外し時認識
300
Ⓐ
カード認識
300a
300b
301a
301b
301
Ⓑ
割り込み要求
302a
302b
302
Ⓒ
リセット

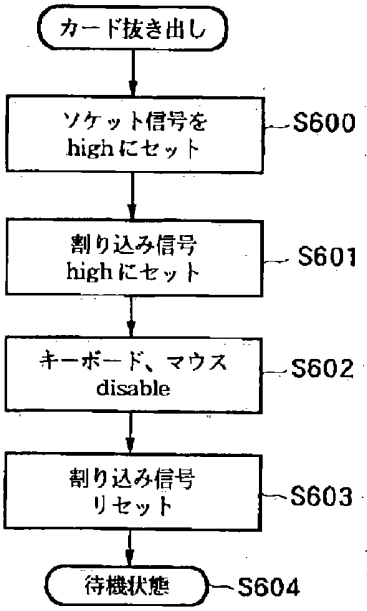
【図４】


カード抜き出し
ソケット信号を
highにセット
S400
割り込み信号
highにセット
S401
サスペンド処理実行
S402
サスペンドフラグ
ONにセット
S403
割り込み信号
リセット
S404
電源OFF
S405
終了

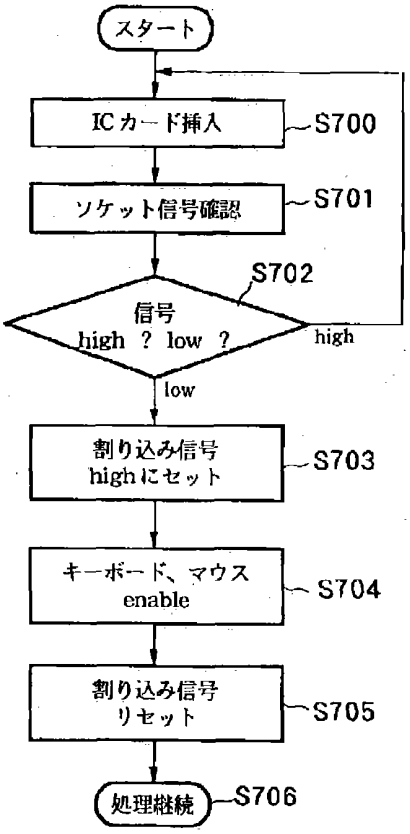
【図５】


スタート
電源ON
S500
ソケット信号確認
S501
S502
信号
high ? low ?
high
low
割り込み信号
highにセット
S503
リジューム処理実行
S504
サスペンドフラグ
リセット
S505
割り込み信号
リセット
S506

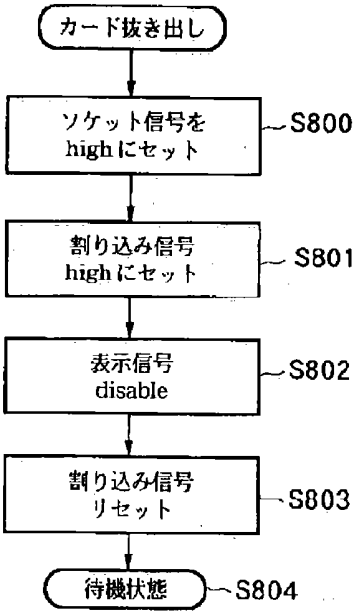
【図６】


カード抜き出し
ソケット信号を
highにセット
S600
割り込み信号
highにセット
S601
キーボード、マウス
disable
S602
割り込み信号
リセット
S603
待機状態
S604

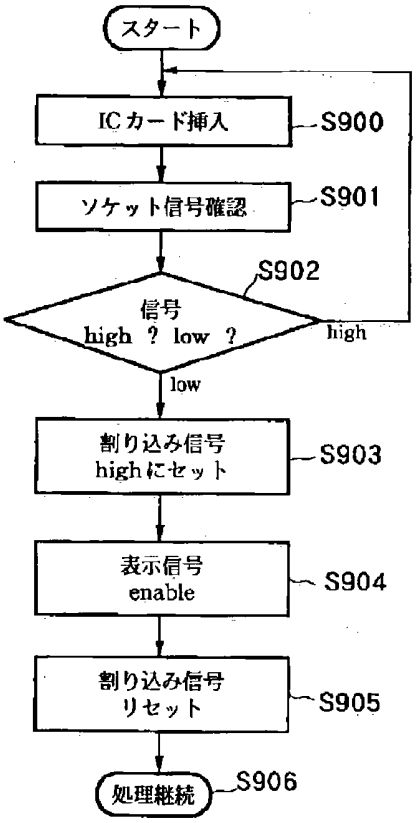
【図7】


スタート
ICカード挿入
S700
ソケット信号確認
S701
S702
信号
high ? low ?
high
low
割り込み信号
highにセット
S703
キーボード、マウス
enable
S704
割り込み信号
リセット
S705
処理継続
S706

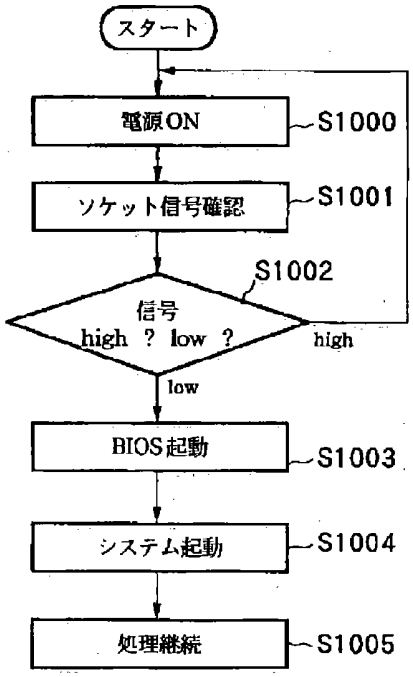
【図８】


カード抜き出し
ソケット信号を
highにセット
S800
割り込み信号
highにセット
S801
表示信号
disable
S802
割り込み信号
リセット
S803
待機状態
S804

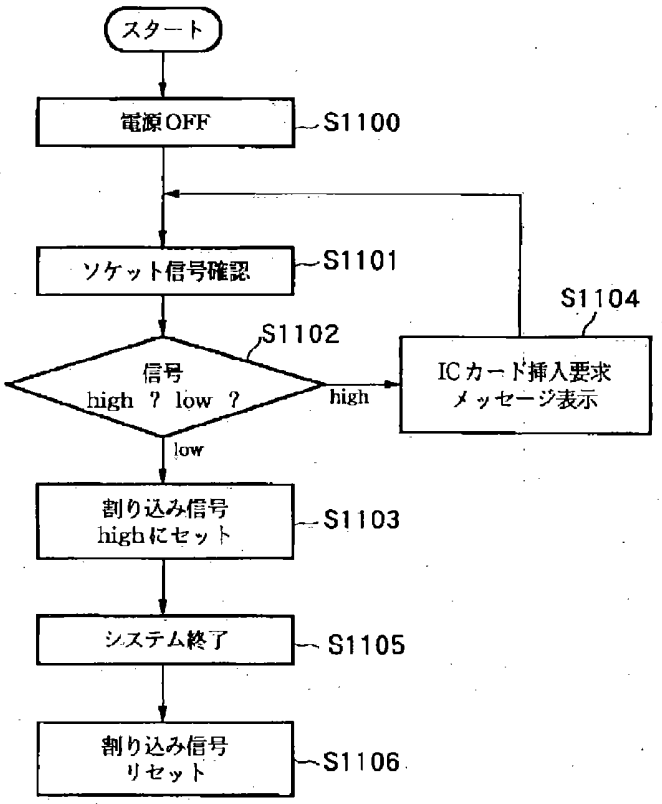
【図９】


スタート
ICカード挿入
S900
ソケット信号確認
S901
S902
信号
high ? low ?
high
low
割り込み信号
highにセット
S903
表示信号
enable
S904
割り込み信号
リセット
S905
処理継続
S906

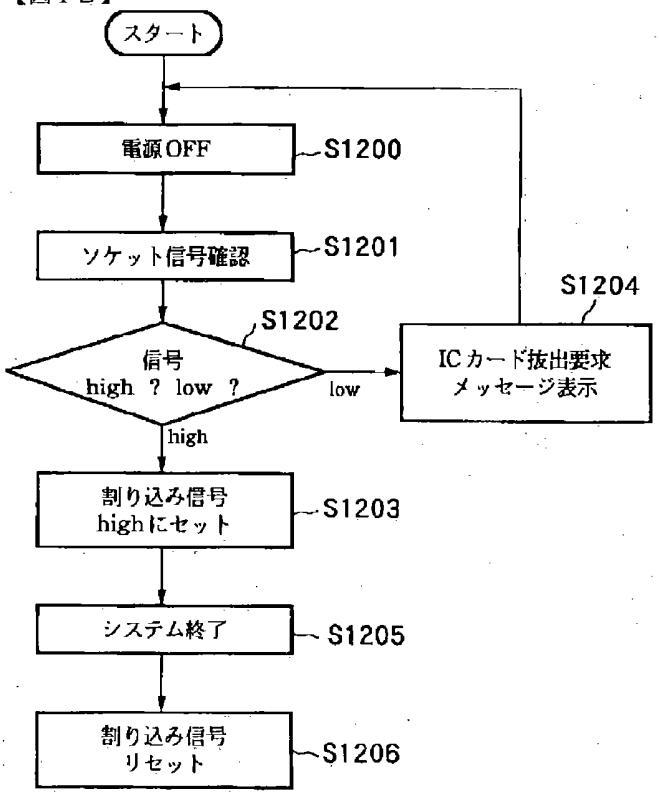
【図１０】


スタート
電源ON
S1000
ソケット信号確認
S1001
S1002
信号
high ? low ?
high
low
BIOS起動
S1003
システム起動
S1004
処理継続
S1005

【図１１】


スタート
電源OFF
S1100
ソケット信号確認
S1101
S1102
信号
high ? low ?
high
S1104
ICカード挿入要求
メッセージ表示
low
割り込み信号
highにセット
S1103
システム終了
S1105
割り込み信号
リセット
S1106

【図１２】


スタート
電源OFF
S1200
ソケット信号確認
S1201
S1202
信号
high ? low ?
low
S1204
ICカード抜出要求
メッセージ表示
high
割り込み信号
highにセット
S1203
システム終了
S1205
割り込み信号
リセット
S1206